U.S. Application No. 09/457,732   15
Docket No. YOR919990137US1
(YOR.080)

REMARKS

Claims 1 and 5-36 are all the claims presently pending in the application.

No claims are amended and no new matter is added. A "clean" listing of the claims is provided for the Examiner's convenience.

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as allegedly not being supported by either a specific and substantial asserted utility or a well established utility.

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 112, first paragraph, as allegedly not being supported by either a specific and substantial asserted utility or a well established invention is not supported by either a specific and substantial asserted utility or a well established utility, and thus, one skilled in the art allegedly would not know how to use the claimed invention.

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as allegedly being inoperative and lacking utility.

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza (U.S. Patent No. 6,446,210) in view of Kharon, et al. (U.S. Patent No. 6,487,662; hereinafter "Kharon").

These rejections are respectfully traversed in the following discussion.

I.   THE CLAIMED INVENTION

The claimed invention provides a method and system of processing semiotic data that allows use of the data <u>without being a threat to privacy and that prevents misuse of such data,</u>

U.S. Application No. 09/457,732   16
Docket No. YOR919990137US1
(YOR.080)

without significantly altering the accuracy and sensitivity of the identification process (e.g.,

see specification at page 3, lines 9-14).

For example, the claimed invention compares encrypted data against stored encrypted

data while at the same time ensuring that unencrypted data is not available or retrievable

under the condition that the data might be slightly different from the template. That is, the

claimed invention determines whether P is close to P' by comparing only h(P) with h(P').

Thus, in contrast to conventional methods, the claimed invention compares encrypted data

against an encrypted template under the possibility that the data might be slightly different

from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17,

and pages 17-20).

II.   REJECTIONS UNDER 35 U.S.C. § 101

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as allegedly not

being supported by either a specific and substantial asserted utility or a well established

utility.

Claims 1, 14-16, 31, and 32 also stand rejected under 35 U.S.C. § 101 as allegedly

being inoperative and lacking utility. That is, the Examiner asserts that the claimed invention

"*could not work*", as evidenced by the Handbook of Applied Cryptography.

Applicants respectfully disagree with each of the Examiner's positions, for the

following reasons.

U.S. Application No. 09/457,732   17
Docket No. YOR919990137US1
(YOR.080)

First, Applicants respectfully submit that the Examiner is misunderstanding the

invention and Applicants' traversal arguments, and has misapplied the teachings of the

Handbook of Applied Cryptography.

For example, the disclosure of the present invention <u>specifically acknowledges</u> the

problem that a simple hash function approach would <u>not</u> work (as suggested by the Examiner

in the Office Action at pages 4-5, numbered paragraph 12)(e.g., see specification at page 16,

lines 15-17).

That is, the specification of the present application (at page 16, lines 15-17)

specifically states that:

> Because $P0$ is in general (possibly) slightly different form Pi for
> $i>0$, the sectret version of $p0$ will generally be quite different from the
> secret version of Pi. This is because cryptographic functions are
> extremely sensitive to the input, thereby to be resilient to attempts to
> decode the encrypted data. In this case, <u>no identification is possible by</u>
> <u>direct comparison of the encrypted data</u> (emphasis added).

Accordingly, the present application discloses several approaches <u>to compare</u>

<u>encrypted or hashed data</u> **under uncertainty** (e.g., see specification at page 16, line 18 to

page 20, line 8).

That is, the specification specifically describes <u>three basis methods **to circumvent**</u>

<u>this situation and the sensitivity of the cryptographic functions</u> (e.g., see specification at

page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe first,

second, and third methods <u>for circumventing the very problem</u> with comparing encrypted or

hash data which the Examiner mentions.

U.S. Application No. 09/457,732   18
Docket No. YOR919990137US1
(YOR.080)

As Applicants have explained in each of the previous Amendments, the claimed

invention compares encrypted data against stored encrypted data while at the same time

ensuring that unencrypted data is not available or retrievable under the condition that the data

might be slightly different from the template. That is, the claimed invention determines

whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16,

lines 12-17, and pages 17-20).

Thus, the present application explains that, in contrast to conventional methods, the

claimed invention compares encrypted data against an encrypted template under the

possibility that the data might be slightly different from the template (e.g., "close" to the

data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

For the foregoing reasons, Applicants respectfully submit that the claimed invention

could (and does) work for its intended purpose, as disclosed in the disclosure of the present

application (e.g., see specification at page 16, lines 12-17, and page 17, line 1, to page 20,

line 8).

With respect to the Examiner's assertion that the claims allegedly are not supported

by either a specific and substantial asserted utility or a well established utility, Applicants

submit that the specification of the present application specifically discloses the utility of the

present application.

For example, the present application specifically states that the claimed invention

provides a method and system of processing semiotic data that allows use of the data without

being a threat to privacy and that prevents misuse of such data, without significantly altering

U.S. Application No. 09/457,732   19
Docket No. YOR919990137US1
(YOR.080)

the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

The specification specifically discloses comparing encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). The specification states that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, contrary to the Examiner's position, Applicants respectfully submit that claims 1, 14-16, 31, and 32: (1) are supported by a specific and substantial asserted utility or a well established utility, (2) are not inoperative and do not lack utility, and (3) could (and do) work for their intended purpose, as disclosed in the disclosure of the specification of the present application, for example, at page 16, lines 12-17, and page 17, line 1, to page 20, line 8.

For the foregoing reasons, Applicants respectfully submit that a person of ordinary skill in the art to which the invention pertains would recognize the utility of the claimed invention and would know and understand the claimed invention. Thus, the Examiner is requested to reconsider and withdraw this rejection.

U.S. Application No. 09/457,732   20
Docket No. YOR919990137US1
(YOR.080)

III.   CLAIM REJECTIONS UNDER 35 U.S.C. § 112, FIRST PARAGRAPH

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 112, first paragraph, as

allegedly not being supported by either a specific and substantial asserted utility or a well

established invention is not supported by either a specific and substantial asserted utility or a

well established utility, and thus, one skilled in the art allegedly would not know how to use

the claimed invention.

As mentioned above, Applicants submit that claims 1, 14-16, 31, and 32: (1) <u>are</u>

<u>supported</u> by a specific and substantial asserted utility or a well established utility, (2) are <u>not</u>

inoperative and do <u>not</u> lack utility, and (3) <u>could (and do) work</u> for their intended purpose, as

disclosed in the disclosure of the specification of the present application, for example, at

page 16, lines 12-17, and page 17, line 1, to page 20, line 8.

Applicants submit that the ordinary skilled artisan could certainly make and use the

claimed invention of a method of processing semiotic data, as claimed, after a thorough

reading of the specification with reference to the drawings.

Applicants note that, as ample case law has held, the test for enablement is whether

<u>one of ordinary skill in the art</u> could practice (e.g., make and use) the invention (e.g., the

claimed invention), <u>without undue experimentation.</u>

Applicants respectfully submit that the specification, drawings, and original claims,

clearly and particularly define the invention with reference, for example, to the exemplary

embodiments (e.g., see specification at page 16, lines 12-17, and page 17, line 1, to page 20,

line 8; see also Figures 1-4 and 6).

U.S. Application No. 09/457,732   21
Docket No. YOR919990137US1
(YOR.080)

In light of the specific examples in the original disclosure, drawings, and claims,

Applicants submit that the ordinarily skilled artisan could certainly make and use the claimed

invention of a method of processing semiotic data after a thorough reading of the

specification with reference to the drawings. In other words, one of ordinary skill in the art

could practice (e.g., make and use) the invention, without undue experimentation.

Thus, Applicants respectfully submit that a person of ordinary skill in the art to which

the invention pertains would recognize the utility of the claimed invention and would know

and understand how to make and use the claimed invention. Therefore, the Examiner is

requested to reconsider and withdraw this rejection.

IV.   THE PRIOR ART REJECTION

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 103(a) as being

unpatentable over Borza in view of Kharon. Applicants respectfully traverse this rejection,

for at least the following reasons.

For the Examiner's convenience, the traversal arguments set forth in the Amendment

under 37 C.F.R. § 1.111 filed on June 18, 2004, the Amendment under 37 C.F.R. § 1.116

filed on January 18, 2005, the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005,

and the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, are incorporated herein

by reference in their entirety.

In the "Response to Arguments" section of the Office Action, the Examiner continues

to allege that the features upon which Applicants rely are not recited in the claims (see Office

Action at page 3, paragraph 5). However, Applicants submit that the traversal arguments

U.S. Application No. 09/457,732   22
Docket No. YOR919990137US1
(YOR.080)

which are set forth at least in the Amendment under 37 C.F.R. § 1.111 filed on April 15,

2005 and the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, clearly point out

the claimed subject matter which is clearly and particularly defined, for example, by

independent claim 1.

Also, in the "Response to Arguments" section of the Office Action, the Examiner

relies on M.P.E.P. § 2122 as stating that, when a reference relied upon expressly anticipates

or makes obvious all of the elements of the claimed invention, the reference is presumed to

be operable.

However, as Applicants have pointed out, Borza does not expressly anticipate or

make obvious all of the elements of the claimed invention. Thus, irrespective of the

operability of Borza, Applicants submit that the alleged combination of Borza and Kharo do

not disclose or suggest all of the features of the claimed invention.

That is, Borza only generally mentions that a comparison of encrypted data is done,

but does not disclose the specific features recited in the claimed invention. In fact, Borza

clearly does not discuss *how* it compares encrypted data.

In fact, the cited portion of Borza at column 16, lines 31-38 does not determine

whether h(P) is close to h(P'), as alleged by the Examiner. Indeed, it is unclear how Borza at

column 16, lines 31-38 even relates to the disclosure of comparing encrypted data against an

encrypted template at column 8, lines 28-38.

That is, nowhere at column 16, lines 31-38, or in Figure 13 which is being described,

does Borza mention comparing encrypted data against an encrypted template. Thus, the

Examiner has mischaracterized the teachings of Borza.

U.S. Application No. 09/457,732   23
Docket No. YOR919990137US1
(YOR.080)

Even assuming *arguendo* that Borza is operative, the disclosure provided by Borza

fails to teach or suggest all of the features of the claimed invention for which it is being

relied upon. Therefore, the alleged combination of Borza and Kharo clearly does not

disclose or suggest all of the features of the claimed invention.

In other words, irrespective of the operability of Borza, the disclosure of Borza

clearly does not disclose or suggest *how* to compare two encrypted data sets to determine

similarity between the two original data sets according to the features recited in the claimed

invention.

Applicants reiterate that the ordinarily skilled artisan would understand that

encryption causes diffusion of data, which means that the encryption of two similar, but not

identical data sets create two encrypted data sets that are very different. Thus, merely

comparing two encrypted data sets still would not (and does not) disclose or suggest the

similarity between the two unencrypted data sets.

In fact, as the Examiner points out, and as Applicants specifically acknowledge in the

specification, no identification is possible by direct comparison of the encrypted data.

Thus, in contrast to Borza, the claimed invention discloses several approaches to

compare encrypted or hashed data **under uncertainty** (e.g., see specification at page 16, line

18 to page 20, line 8).

Specifically, as mentioned above, the disclosure of the present invention specifically

acknowledges the problem that a simple hash function approach would not work (as

suggested by the Examiner in the Office Action at pages 4-5, numbered paragraph 12)(e.g.,

see specification at page 16, lines 15-17).

U.S. Application No. 09/457,732   24
Docket No. YOR919990137US1
(YOR.080)

For example, the specification of the present application (at page 16, lines 15-17)

specifically states that:

> Because *P0* is in general (possibly) slightly different form *Pi* for
> *i>0*, the sectret version of *p0* will generally be quite different from the
> secret version of *Pi*. This is because cryptographic functions are
> extremely sensitive to the input, thereby to be resilient to attempts to
> decode the encrypted data. In this case, no identification is possible by
> direct comparison of the encrypted data (emphasis added).

Accordingly, the present application discloses several approaches to compare

encrypted or hashed data under uncertainty (e.g., see specification at page 16, line 18 to

page 20, line 8).

That is, the specification specifically describes three basis methods to circumvent

this situation and the sensitivity of the cryptographic functions (e.g., see specification at

page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe first,

second, and third methods for circumventing the very problem with comparing encrypted or

hash data which the Examiner mentions.

The claimed invention compares encrypted data against stored encrypted data while at

the same time ensuring that unencrypted data is not available or retrievable under the

condition that the data might be slightly different from the template. That is, the claimed

invention determines whether P is close to P' by comparing only h(P) with h(P') (e.g., see

specification at page 16, lines 12-17, and pages 17-20).

The present application explains that, in contrast to conventional methods, the

claimed invention compares encrypted data against an encrypted template under the

U.S. Application No. 09/457,732   25
Docket No. YOR919990137US1
(YOR.080)

possibility that the data might be slightly different from the template (e.g., "close" to the

data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, the claimed invention solves the problem that a simple hash function approach

would _not_ work (as suggested by the Examiner in the Office Action at pages 4-5, numbered

paragraph 12)(e.g., see specification at page 16, lines 15-17) by circumventing the problem,

as disclosed and claimed.

For the foregoing reasons, Borza clearly does _not_ disclose or suggest at least "*to*

determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s

to determine whether P' substantially matches, but does not exactly match, one of said data

set P", as recited in claim 1.

On the other hand, Applicants respectfully reiterate that Kharon does _not_ make up for

the deficiencies of Borza.

The Examiner relies on Kharon for teaching the claimed "*extracting sub-collections*

Sj from the collection of data in data set P; encrypting a predetermined number of such sub-

collections such that at least one of the sub-collections is reproduced exactly with a

predetermined probability, comparing encrypted versions of the sub-collections Sj with those

data stored in said database, wherein if one or more of the sub-collection Sj matches with

said data, then verification is deemed to have occurred", as recited in independent claim 1.

However, contrary to the Examiner's position, Kharon (at column 13, lines 43-67)

does _not_ describe extracting _multiple_ subsets Sj (i.e., "*sub-collections*") from the data.

Furthermore, Kharon does _not_ describe encrypting a _number of such subsets_ (i.e., a "*number*

U.S. Application No. 09/457,732   26
Docket No. YOR919990137US1
(YOR.080)

of such sub-collections") such that at least one is reproduced exactly with a predetermined

probability.

Applicants respectfully submit that the Examiner seems to have confused using a

smaller section of the data for verification (which would be less desirable since less data is

used), whereas the claimed invention uses <u>multiple subsets</u> of the data for verification.

Thus, using just a <u>smaller subset</u> of the data for verification would be <u>less</u> desirable

since it is easy to forge the data and does <u>not</u> solve the problem of being able to <u>compare two</u>

<u>encrypted data</u>.

On the other hand, using <u>multiple subsets</u> of the data, according to the claimed

invention, <u>allows encrypted data to be compared and to generate a measure of similarity</u>.

Thus, for the foregoing reasons, Applicants respectfully reiterate that neither Borza

nor Kharon discloses or suggests all of the features of the claimed invention. Therefore, the

Examiner is requested to reconsider and withdraw this rejection.

V.   CONCLUSION

In view of the foregoing, Applicants submit that claims 1 and 5-36, <u>all</u> the claims

presently pending in the application, are patentably distinct over the prior art of record and

are in condition for allowance. The Examiner is respectfully requested to pass the above

application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance,

the Examiner is requested to contact the undersigned at the local telephone number listed

below to discuss any other changes deemed necessary in a telephonic or personal interview.

U.S. Application No. 09/457,732   27
Docket No. YOR919990137US1
(YOR.080)

The Commissioner is hereby authorized to charge any deficiency in fees or to credit

any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: _December 16, 2005_   _____
John J. Dresch, Esq.
Registration No. 46,672

Sean M. McGinn, Esq.
Registration No. 34,386

**MCGINN INTELLECTUAL PROPERTY
 LAW GROUP, PLLC**
8321 Old Courthouse Road, Suite 200
Vienna, Virginia 22182-3817
(703) 761-4100
Customer No. 21254

CERTIFICATE OF TRANSMISSION

I certify that I transmitted via facsimile to (571) 273-8300 the enclosed Request for

Reconsideration under 37 C.F.R. § 1.111 to Examiner Christian A. La Forgia on December

16, 2005.

_____
John J. Dresch, Esq.
Registration No. 46,672
Sean M. McGinn, Esq.
Registration No. 34,386